УДК 004.056

Бурячок В.Л., Корченко О.Г., Бурячок Л.В.

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК МЕТОД РОЗВІДКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Стрімкий технологічний розвиток інформаційного суспільства веде до зростання обсягу інформації, що циркулює, накопичується та обробляється в інформаційному і кіберпросторах. Це потребує розроблення нових (удосконалювання існуючих) способів і методів пошуку та збору інформації у відкритих, відносно відкритих закритих електронних джерелах. Вирішення цих завдань можливо в межах такого перспективного виду діяльності, як розвідка інформаційно-телекомунікаційних систем (ІТС), комплексного дослідження якого ні вітчизняними, ні зарубіжними фахівцями до цього часу не проводилось. На підставі аналізу відкритих джерел розкрито основні аспекти, особливості, способи і методи проведення розвідки ІТС та визначено, що вона буде визнана найефективнішим засобом виявлення, профілактики, протидії та боротьби з найрізноманітнішими кібернетичними втручаннями і загрозами. Констатовано, що найбільш дієвим і потужним способом розвідки ІТС на найближчу перспективу залишатиметься кіберрозвідка, призначена для пошуку та збору розвідувальної інформації передусім у Internet, а найбільш результативним – метод соціальної інженерії, призначений для організації доступу до будь-яких найзахищеніших інформаційних ресурсів.

Ключові слова: соціальна інженерія,кіберрозвідка, кіберрозвідка в інформаційно-телекомунікаційних системах, розвідка ІТС, кіберпростір, кібернетичний простір.

Наприкінці XX початку XXI сторіччя завдяки глибоким системним перетворенням, викликаним синтезом перспективних інформаційно-комунікаційних технологій (ІКТ) і бурхливим розвитком інформаційно-телекомунікаційних систем (ІТС), поступово почали формуватись принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний і кібернетичний простори. Поступово вони накопичили практично необмежений потенціал і нині, за рахунок забезпечення оброблення і передавання їх головного об'єкта – інформації, відіграють суттєву роль в економічному та соціальному розвитку будь-якої країни світу.

Про важливість інформаційного і кіберпросторів свідчить поява концепцій ведення боротьби у них, а також створення у Збройних силах багатьох країн світу спеціальних структур, призначених для ведення такої боротьби. Такий стан справ, а також глибинні зміни у відношенні більшості держав земної кулі до власної інформаційної й, як наслідок, кібернетичної безпеки фактично зумовлюють необхідність розроблення рекомендацій щодо коротко- та довгострокових пріоритетів трансформації безпекового сектору цих держав, зокрема України за такими напрямами:

- пошук і добування інформації у відкритих та відносно відкритих джерелах про можливості протиборчих сторін, а також обмін нею;
- захист власного інформаційного ресурсу від внутрішніх і зовнішніх, навмисних або випадкових кібернетичних втручань і загроз.

Цю проблему висвітлено в багатьох публікаціях зарубіжних і вітчизняних авторів. Найвідомішими серед них є роботи В.В. Домарєва, Дж. Козіола [4], М. Кузнєцова [5], Кр. Касперськи [7], К. Митника, І. Симдянова та інших фахівців. Проте аналіз публікацій у предметній області, що розглядається, свідчить, що комплексного дослідження проблеми, перш за все розвідки ІТС, а також методів, які при цьому застосовуються, та їх особливостей сьогодні немає. Тому вона потребує додаткового і більш глибокого вивчення.

Отже, актуальність статті передусім зумовлено обсягом інформації, що останнім часом надходить до користувачів із зовнішнього середовища та безперервно зростає; а також потребою підвищення ефективності засобів пошуку і добування інформації про об'єкти розвідки із ресурсів ІТС та адекватного оцінювання на її підставі можливих загроз власному інформаційному і кіберпросторам.

Важливою умовою вирішення означених проблем стає оперування єдиним понятійним апаратом у цій царині, а також знання специфіки розвідувальних процесів у ІТ середовищі та поведінки у ньому так званого когнітивного базису [1] – звичайних користувачів, професійних шпигунів та/або хакерів (порушників тощо). Тому мета статті та її основний зміст саме й полягають у викладенні основних понять і особливостей розвідки ІТС

й кіберрозвідки зокрема, як одного з основних способів її проведення, а також методів, що використовуються для цього – передусім соціальної інженерії, яка базується на знанні психологічних особливостей суб'єкта розвідки.

Під розвідкою ІТС розумітимемо [2, 3] комплекс заходів, спрямованих на систематичний і цілеспрямований пошук та добування з ІТС інформації стосовно протиборчої сторони (конкурента), її вивчення та оброблення, а також формування на цій підставі уявлення про реальні та/або потенціально можливі джерела деструктивного впливу на власний кіберпростір. Від інших видів розвідка ІТС відрізняється перш за все механізмами (способами і методами), а також силами і засобами, що задіяні в добуванні розвідувальної інформації. Головними способами ведення розвідки ІТС (рис. 1) вітчизняні та закордонні фахівці нині вважають розвідку систем телекомунікацій (РсТ), мережеву розвідку (МР) і кіберрозвідку (КР).

Рис. 1. Способи ведення розвідки ІТС

Ці способи забезпечують систематичний пошук, збір та добування:

- інформації (знаків, сигналів, звуків, зображень і текстових повідомлень будь-якого роду) про об'єкти розвідки у захищених системах її передавання, випромінювання та/або приймання (РсТ), а також у відкритих і відносно відкритих електронних джерелах (КР);
- даних про ресурси, засоби захисту, пристрої та програмне забезпечення (ПЗ), що використовується в ІТС об'єкта розвідки, їх уразливі місця та межі проникнення (МР), – з подальшим обліком та накопиченням такої інформації/даних, її верифікацією, вивченням та аналітичним обробленням.

Зважаючи на те що силами і засобами РсТ та МР добувається відповідно до 5–8 % та до 7 % інформації, яка необхідна протиборчим сторонам одна про одну, останнім часом надзвичайно розвинувся такий спосіб розвідки ІТС, як КР. Її силами і засобами нині може добуватися від 35 % до 95 % інформації про об'єкти розвідки, яка має властивість не тільки не відрізнятися від військових і державних таємниць, але й часто перевершувати їх за своєю цінністю. Залежно від важливості та специфіки покладених завдань, наявних ресурсів, а також за методами, що застосовуються для пошуку і збору інформації [2], кіберрозвідка ІТС поділяється на технічний і програмний методи її ведення, метод так званої соціальної інженерії (СІ), а також метод, що передбачає моніторинг відкритих і відносно відкритих електронних джерел (рис. 2).

Рис. 2. Складові кіберрозвідки

Серед них саме завдяки людському чиннику в умовах стрімкого розвитку мережі Internet можуть бути подолані такі відомі технології безпеки, як міжмережеві екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережевих атак тощо.

Зважаючи на таке західні і вітчизняні фахівці саме метод СІ (від англ. Social Engineering) вважають одним із найбільш перспективних методів КР [4–6]. На їх думку він полягає в одержанні неавторизованим користувачем (хакером, порушником тощо) несанкціонованого доступу до інформації про призначення, структуру, встановлені права доступу, систему захисту, реєстраційні імена і паролі, а також іншої конфіденційної інформації про об'єкт атаки – людину (або групу людей), використовуючи її (їх) слабкість або некомпетентність, непрофесіоналізм або недбалість та керуючи її (їх) діями. Метод може практикуватись як самостійно, без застосування технічних засобів [1], так і бути інструментом під час планування та проведення інших видів атак на об'єкт розвідки із застосуванням закладених пристроїв та/або програмних закладок.

Технологіями СІ людство в тій чи іншій формі користувалось з давніх-давен. Так, наприклад, у Римській імперії вшановували людей, які вміли ввести співрозмовника в оману та впевнити його у правоті того, чого не могло бути. Прикриваючись високими посадами своїх покровителів й виступаючи від їх імені, вони, використовуючи вигідні аргументи, підлещування або завуальовану дезінформацію, вели дипломатичні переговори й були здатні вирішити певні питання не тільки особистого, а й державного рівня. Тобто, ще тоді спрацьовувала приказка: "… найслабкіша ланка системи безпеки – людина …". У сучасному розумінні поняття СІ з'явилось досить недавно. Вперше його ввів Кевін Митник, який стверджував, що набагато простіше довідатись про чийсь пароль для доступу, ніж зламувати всю систему цілком. Враховуючи таке технології СІ порушники найчастіше використовують нині для таких цілей:

- збору довідкової інформації про об'єкт атаки (розвідки), а саме з'ясування інтересів та особливостей поведінки потенційної жертви, чатів і форумів якими вона користується, а також імен, під якими вона з'являється у мережі Internet шляхом ведення діалогу з нею або з її оточенням у службах обміну миттєвими повідомлення (messenger), наприклад, ICQ;
- одержання закритої (конфіденційної) інформації про об'єкт атаки (розвідки) або інформації, що становить для порушника певний інтерес, наприклад, номери телефонів потенційної жертви, адресу її прописки/проживання, реальне ім'я і прізвище та іншої подібної інформації шляхом встановлення контакту з нею та/або уведення її в оману;
- одержання інформації про об'єкт атаки (розвідки), що необхідна для забезпечення несанкціонованого доступу до системи, а саме пароля, яким користується потенційна жертва, серії й номеру її паспорта та інших відомостей про неї шляхом входження до жертви у довіру;
- примушення об'єкта атаки (розвідки) до дій, необхідних порушнику шляхом нав'язування такому об'єкту нової моделі поведінки.

Для цього вони застосовують зокрема такі види атак, як введення в оману (поєднуються прийоми видавання себе за іншу особу, відволікання уваги, створення умов для психологічного перевантаження), розсилання спама (наприклад, комерційної, політичної та іншої реклами або повідомлень іншого роду особам, які не виявляють бажання їх отримувати), спонукання до звернення про допомогу у вирішенні певних проблем (обернена СІ, рис. 3), прямий або опосередкований шантаж, користуючись такими методами, як:

- претекстінг (дії, що в ході атаки, здійснюваної зазвичай по телефону, відпрацьовуються порушником за заздалегідь сформованим сценарієм і мають на меті забезпечити його входження у довіру до жертви);
- фішинг або так зване електронне шахрайство (дії, що в ході атаки, здійснюваної порушником через e-mail, вимагають від потенціальної жертви розголосити певну

конфіденційну інформацію про себе – логіни, паролі тощо шляхом її так званої перевірки);

- несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи;
- запуск злоякісного ПЗ, наприклад, троянських програм (бекдорів, руткітів, кейлогерів, клікерів та проксі-троянів) як відповіді на e-mail запит порушника або через інфікований CD (флеш-накопичувач) тощо.

Рис. 3. Принцип оберненої соціальної інженерії

Прикладом такому можуть слугувати троянський proxy-сервер “Mitglieder” та ICQ-черв’як “Bizex”, що з’явилися у 2004 році [7, 8]. Перший з них проникав до комп’ютера-жертви через уразливість у Microsoft Internet Explorer, яка дозволяла встановити і запустити proxy-сервер на зараженій машині без відома користувача. Після зараження відкривався порт, що використовувався для розсилання спаму. Таким чином, заражені машини утворювали мережу машин-зомбі (ботнет), якими можна було керувати віддалено. Для поширення ICQ-черв’яка “Bizex” порушники використовували масове несанкціоноване розсилання по ICQ повідомлення “http://www.jokeworld.biz/index.html:)) LOL”. Одержавши таке повідомлення об’єкт атаки, що нічого не підозрював, відкривав зазначену сторінку й у випадку, якщо використовувався браузер Internet Explorer з незакритою уразливістю, на комп’ютер завантажувалися файли черв’яка, а в деяких випадках і супутнього йому трояна. Після установки в систему “Bizex” закривав запущений ICQ-клієнт і, підключившись до сервера ICQ з даними зараженого користувача, розсилав спам за знайденими на комп’ютері списками контактів. Одночасно відбувалася крадіжка конфіденційної інформації – банківських даних, логінів і паролів тощо. Алгоритм дій порушників (рис. 4) базувався при цьому на особливостях прийняття рішень звичайними користувачами, професійними шпигунами та/або хакерами, яких у західних інформаційних джерелах нині називають когнітивним базисом [3].

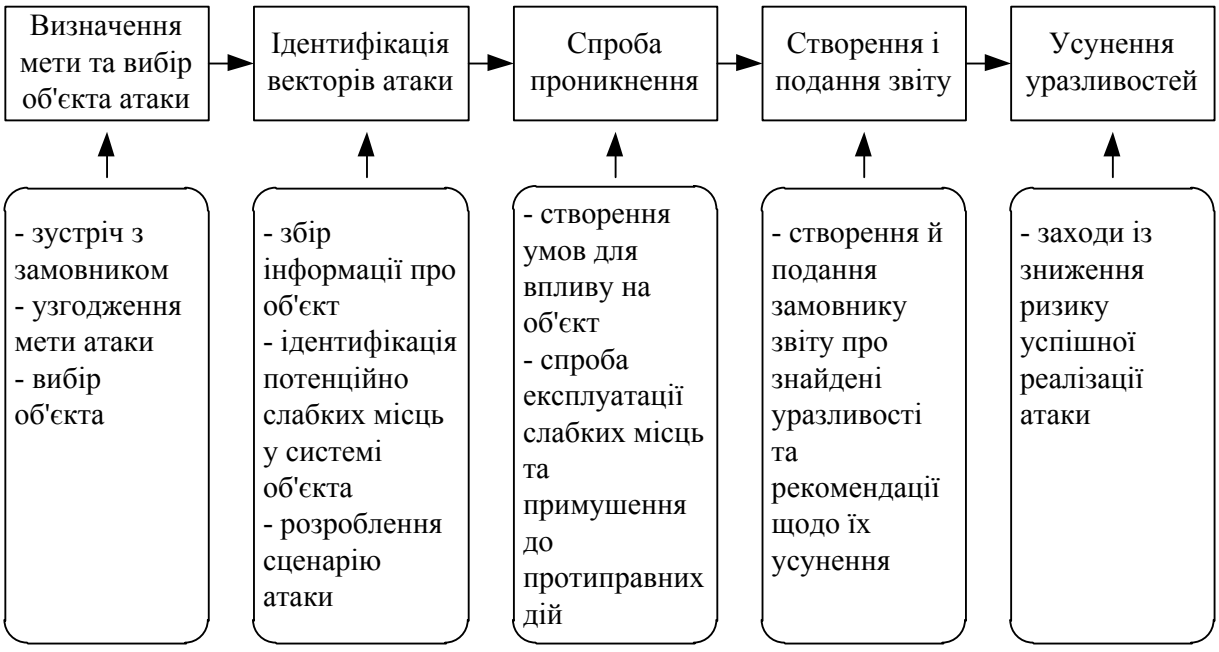

Рис. 4. Алгоритм дій порушників методом соціальної інженерії

У цей час, розробивши сценарій атаки, порушники використовують такі основні компоненти ПЗ, як, наприклад, повідомлення, яке в свою чергу складається з інформаційного наповнення, відомостей про відправника й довідкового посилання на злоякісне ПЗ та засіб доставки (електронну пошту, службу миттєвих повідомлень та/або однорангові мережі). Застосування інформаційного наповнення повідомлення в атаках методом СІ, перелічених вище вважається, порівняно з іншими складовими такого повідомлення, найбільш ефективним. Його перевага полягає в тому, що атака фактично завжди буде вдалою, якщо порушник здатний сформулювати текст повідомлення таким чином, щоб зацікавити потенціальну жертву й примусити її його відкрити.

Зважаючи, що більшість користувачів Internet працює нині переважно з електронною поштою, для розповсюдження повідомлень з деструктивним інформаційним наповненням порушники останнім часом частіш за все використовують саме цей канал. Його можливості одними з перших наприкінці минулого століття реалізували розробники вірусів “Melissa” та “LoveLetter”. Через електронну пошту віруси надсилали власні копії користувачам, адреси яких вибирались з адресної книги інфікованого комп’ютера, з ознакою важливого повідомлення та певним змістом (рис. 5). У результаті таких дій інфікованими виявлялись, як правило, всі комп’ютери, власники яких зацікавились цим повідомленням.

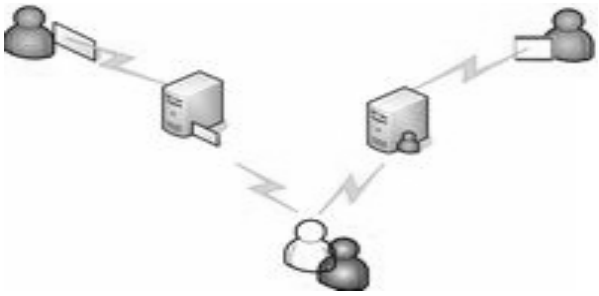

Рис. 5. Структурно-логічна схема дій порушника з використанням можливостей електронної пошти та служби миттєвих повідомлень

Окрім цього для розповсюдження вірусу “LoveLetter” розробники започаткували методику так званих подвійних розширень файлів:

<назва файлу>. <фальшивка з розширенням, що не викликає підозру>. <реальне розширення файлу>. Наприклад, ILOVEYOU.txt.vbs.

Все це дає підстави стверджувати, що повністю позбутися атак на рівні ПЗ методом СІ нині неможливо, але їх негативні наслідки можна зменшити за рахунок:

- вивчення слабких місць прикладного ПЗ на підставі даних корпорацій CERT та Bugtrad (http://www.cert.com та http://www.securityfocus.com відповідно);
- застосування, крім системного адміністрування системи розпізнавання атак (IDS), технологій, що їх взаємодоповнюють та надають можливість відстежувати всі пакети, які проходять через мережевий інтерфейс;
- дослідження спеціальних аналітичних додатків із застосуванням log-файлів операційних систем та мережевих log-файлів тощо.

Ще одним з різновидів атак методом СІ, використовуваних порушниками для одержання спеціальної інформації з ІТС, нині вважається створення підставних профілів. Найбільш відомим прикладом цьому було створення Томасом Райаном з Provide Security підставного профілю молодої симпатичної дівчини 25 років, яка за легендою була фахівцем з 10-річним стажем роботи в сфері безпеки, закінчила престижний коледж у Нью-Хемпширі й мала вчений ступінь. Від імені свого віртуала Томас через популярні соціальні сервіси Facebook, LinkedIn і Twitter відправив запити на додавання в друзі 300 чоловікам і жінкам із числа військових, співробітників секьюриті-компаній і державних чиновників. Згодом

віртуальну дівчину стали запрошувати на конференції з питань безпеки, а великі компанії типу Google і Lockheed Martin взагалі висловили бажання найняти її на роботу. Через деякий час після початку активного життя її почали самостійно додавати в друзі інші люди – колеги тих, кому "спеціалістка у сфері безпеки" нав'язала своє спілкування першою. У такий спосіб Томас Райан одержав доступ до великої кількості особистої інформації (персональних даних), фотографій, а також розкрив зв'язки спілкування певних фахівців, що становили для нього певний інтерес.

Але, як виявляється, СІ не вичерпується одними лише соціальними мережами. Прикладом цьому став конкурс, проведений на одній з конференцій Defcon, у ході якого всім бажаючим було запропоновано за один дзвінок тривалістю у 25 хвилин витягнути максимум інформації, що сприяла б організації успішної кібератаки. Один з учасників конкурсу зумів за допомогою всього двох телефонних дзвінків ввести в оману співробітника технічної підтримки компанії British Petroleum та змусити його видати інформацію, яка б допомогла в організації кібератаки на цю фірму. Серед отриманих ним відомостей були дані про те, які моделі ноутбуків використовують співробітники British Petroleum, а також які операційні системи, браузери, антивіруси й програми для організації VPN установлені на цих комп'ютерах. Крім того, переможець примусив співробітника British Petroleum відвідати сайт Social-Engineer.org, завдяки чому заробив ще декілька додаткових балів.

Крім цього доволі відомими є випадки, коли хакери отримували нагоду проникнути до ІТС об'єкта розвідки за результатами вивчення вмісту сміттєвих ящиків, наприклад, у Нью-Йоркській телефонній компанії, або ж шляхом виявлення слабких місць у системі мережної безпеки. Одним з таких місць у мережі банку BABank (США) виявилось закриття порта технічного обслуговування паролем, встановленим виробником [2]. Як результат хакери отримали всі права доступу до системи. У подальшому внаслідок використання на поштовому сервері застарілої версії Unix хакери встановили над цим сервером контроль і отримали змогу взаємодіяти з іншими серверами на адміністративному рівні.

На підтвердження можливостей СІ компанія Check Point Software Technologies – розробник ПЗ, призначеного для забезпечення інформаційної безпеки, у 2011 році провела дослідження під назвою "Ризики соціальної інженерії в контексті інформаційної безпеки". Її фахівці у ході опитування 853 ІТ-професіоналів і спеціалістів з інформаційної безпеки, які представляли провідні компанії США, Великобританії, Канади, Австралії, Нової Зеландії та Германії зробили висновок, що понад 43 % бізнес структур протягом останніх двох років зазнали цільових атак методом соціальної інженерії, кожна з яких потенціальній жертві обійшлася приблизно у 25–100 тисяч доларів. Майже 70 % усіх порушень, пов'язаних з безпекою інформації, здійснювалось саме співробітниками цих структур. Майже третина з досліджених респондентів була атакована 25 і більше разів і лише 16 % з них заявили, що СІ їх не турбує. За результатами опитування з'ясувалось, що найбільш розповсюдженими джерелами загроз соціальних злочинців є фішингові листи (47 % респондентів), соціальні мережі (39 %), а також незахищені мобільні пристрої (12 %). Більша частина учасників дослідження (86 %) заявила, що вони усвідомлюють ризики, пов'язані з людським фактором. Разом з тим лише частина з них (26 %) засвідчила, що регулярно проводять відповідні тренінги для персоналу або планують розроблення відповідної програми (19 %), а 40 % відсотків респондентів взагалі усю відповідальність за можливі витоки покладають саме на персонал.

Для захисту користувачів від СІ фахівці компанії рекомендували застосовувати як організаційні (на рівні установи, організації), так і програмно-технічні засоби [6, 7]. До організаційних засобів забезпечення захисту інформації нині належать організаційно-технічні (підготовка приміщень з ПЕОМ, прокладання кабельної системи з урахуванням

вимог щодо обмеження доступу тощо) та організаційно-правові (вимоги національного законодавства тощо) засоби. Їх перевага обумовлюється можливістю вирішення різних проблем, простотою реалізації та необмеженими можливостями модифікації і розвитку.

Головний недолік – висока залежність від суб'єктивних факторів. До технічних (апаратних) засобів належать різні за типом пристрої, які або заважають фізичному проникненню на об'єкт розвідки (захисна сигналізація тощо), або виявляють і перекривають потенціальні канали витоку інформації (генератори шуму, мережеві фільтри, скануючі радіоприймачі тощо). Їх переваги обумовлюються надійністю, незалежністю від суб'єктивних факторів та високою стійкістю до модифікації. Основним недоліком, як правило, є вартісний аспект. До програмних засобів належать програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення тимчасових файлів тощо. Їх переваги полягають в універсальності, гнучкості, надійності, здатності до модифікації і розвитку. Недоліки обумовлюються обмеженою функціональністю мережі, використанням частини ресурсів файл-сервера та автоматизованих робочих місць (робочих станцій), чутливістю до випадкових і спланованих змін, можливою залежністю від типів ПЕОМ тощо.

Висновки:

1. Соціальна інженерія є одним із напрямів хакінгу за участю якого, зважаючи на простоту реалізації, відносну складність виявлення, незначні фінансові вкладення та мінімальний ризик провалу, нині відбувається майже 70 % несанкціонованих проникнень до ІТС і мереж.

2. На відміну від SQL-ін'єкцій, застосування експлойтів, вірусів, переповнення буфера, DoS і DDoS-атак, бекдорів, руткітів та інших методів проникнення й виведення систем з ладу, – атака методом СІ дає можливість порушникам отримати практично стовідсотковий ефект у разі доступу до найзахищеніших інформаційних ресурсів об'єкта атаки.

3. Застосовуючи соціальну інженерію сумісно з деперсонофікованими центрами Internet-доступу, портативною ЕОТ, сертифікованими базами даних/знань пошукових матеріалів та джерел інформації тощо, розвідувальні підрозділи матимуть можливість:

- викривати ознаки підготовки протиборчих сторін до збройного нападу, визначати порядок їх ходів та очікувані виграші;
- відстежувати всі етапи проходження інформації, що циркулює в ІТС;
- уникати ускладнень у ході пошуку та оброблення інформації, а також її накопичення та зберігання тощо.

4. Типових заходів протидії атакам методом соціальної інженерії нині, на жаль, не існує. Кожна ситуація потребує індивідуального підходу і всебічного вивчення.

5. Оскільки інформаційна і кібербезпека – неперервний процес, досить важливим для забезпечення максимального захисту організації (установи) від внутрішнього і зовнішнього, випадкового і навмисного деструктивного впливу є привертання уваги персоналу до питань безпеки, додержання персоналом вимог впровадженої в організації (установі) політики безпеки та застосування персоналом у роботі низки методів і дій, необхідних для підвищення захисту інформаційного забезпечення.

ЛІТЕРАТУРА

1. В. Бычек. Социальная инженерия в интеллектуальной битве "добра" и "зла". / В. Бычек, Е. Єршова // [Електронний ресурс]. – Режим доступу: http://www.aladdin-rd.ru/company/pressroom/articles/11475/ .
2. Бурячок В.Л. До питання організації та проведення розвідки у кібернетичному просторі. / Бурячок В.Л., Гулак Г.М., Хорошко В.О. // Наука і оборона. – 2011. – №2. – С. 19– 23.
3. Бурячок В.Л. Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу / В.Л. Бурячок, О.А. Ільяшов, Г.М. Гулак. // Збірник матеріалів круглого столу "Актуальні питання підготовки фахівців із розслідування кіберзлочинів", 25.11.2011. – К.: Наук.-вид. відділ НА СБ України, 2011. – С. 27–32.

4. Козиол Дж. Искусство взлома и защиты систем. / Дж. Козиол, Д. Личфилд, Д. Эйтэл, К. Энли и др. // .– СПб: Питер, 2006. – 416 с: ил.
5. М. Кузнецов. Социальная инженерия и социальные хакеры. / М. Кузнецов, И. Симдянов. // – Петербург: БХВ-Петербург, 2007. – 368 с.
6. Крис Касперски. Секретное оружие социальной инженерии. [Електронний ресурс]. – Режим доступу: http://kpnc.opennet.ru/SOC_ENG.pdf.
7. [Електронний ресурс]. – Режим доступу: ru.wikipedia.org
8. Современные угрозы и каналы утечки информации в компьютерных сетях. [Електронний ресурс]. – Режим доступу: http://bibliofond.ru/view.aspx?id=67579.

Надійшла: 18.10.2012 р.

Рецензент: д.т.н., професор Хорошко В.О.

УДК 004.627(045)

Гумен М.Б., Юдін О.К., Курінь К.О.

ТЕХНОЛОГІЯ СТИСНЕННЯ НА БАЗІ МЕТОДУ КОДУВАННЯ ДВІЙКОВИХ ПОСЛІДОВНОСТЕЙ ЗА КІЛЬКІСТЮ БІТОВИХ ПЕРЕХОДІВ

Запропоновано технологію стиснення зображень на базі методу кодування за кількістю бітових переходів. Сформовано прототип технології стиснення зображень. Обґрунтовано вибір методу трансформації вихідного зображення. Обґрунтовано вибір методу кодування квантованих трансформант зображення. Розроблено структурну модель процедури стиснення зображень з урахуванням методу кодування за кількістю бітових переходів.

Ключові слова: структурне кодування, стиснення зображень, дискретне вейвлетне перетворення, квантування, структурні ознаки

Вступ. Інформаційно-комунікаційні системи та мережі (ІКСМ) в сучасних умовах розвитку суспільства все ширше застосовують графіку різних класів. Так, наприклад, неможливо уявити висвітлення наукових результатів, а також жодних комунікаційних послуг в ІКСМ без роботи прикладного програмного забезпечення з графічними інтерфейсами різних типів. Деякі здійснювані інформаційною системою найпростіші дії, наприклад завантаження та пересилка файлів, також відображуються графічно. Більшість програм пропонують користувачеві графічний інтерфейси типу GUI, який значно спрощує роботу користувача й дозволяє легко інтерпретувати отримані результати. Комп'ютерна графіка використовується в багатьох областях повсякденної діяльності при перетворенні складних масивів даних в графічне відображення. Отже, графічні зображення вкрай важливі, але вони вимагають великих об’ємів пам’яті. Оскільки сучасні дисплеї передають безліч кольорів, кожен піксел прийнято інтерпретувати у вигляді 24-бітового числа, в якому компоненти червоного, зеленого й блакитного кольорів займають по 8 біт кожен. Такий 24-бітовий піксел може відтворює мільйонів кольорів. Зрозуміло, що стандартні зображення з розміром 512×512 пікселів займатимуть 786432 байтів, а зображення розміром 1024×1024 пікселів буде вимагати 3145728 байт для його зберігання. Анімація, яка також широко застосовується в комп'ютерних додатках, вимагає ще більшого об'єму пам’яті. Все це пояснює важливість використання сучасних технологій та методів стиснення зображень.

Постановка завдання досліджень.

Одними з найпоширеніших на сьогоднішній день кодерів стиснення зображень є технології типу JPEG та JPEG-2000, що розроблялися об'єднаною міжнародною групою експертів з обробки відеозображень (Joint Photographic Experts Group) для стиснення неперервнотонових зображень. Обидві ці технології базуються на методах кодування, які враховують статистичну надмірність даних. Дані алгоритми стиснення мають наступні недоліки [1]:

- можливі втрати інформації, які виникають на етапах дискретних перетвореннь та квантування компонент зображення;
- залежність ефективності стиснення від характеристик джерела інформації;